AE

(12) UK Patent Application (19) GB (11) 2 294 720 (13) A

(43) Date of A Publication 08.05.1996

(21) Application No 9418887.7

(22) Date of Filing 20.09.1994

(51) INT CL^6
E05B 49/00 // E05B 19/00

(52) UK CL (Edition O)
E2A AEE

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition O) E2A AEE
INT CL^6 E05B 19/00 49/00
Online: WPI

(71) Applicant(s)
Nigel Janson
21 Clevedon Road, Failand, BRISTOL, BS8 3UG, United Kingdom

(72) Inventor(s)
Nigel Janson

(74) Agent and/or Address for Service
Nigel Janson
21 Clevedon Road, Failand, BRISTOL, BS8 3UG, United Kingdom

(54) A transponder key holder

(57) A transponder key holder 18 for use by security systems in which a key transponder 15 is provided with a stored electronically readable code that can be detected upon approach or insertion of the key to a lock. The key-holder provides a means by which the coded information is protected from unauthorised code reading by way of an electromagnetic shield as part of the key body and holder and by a second transponder 21 that serves to interfere with the electromagnetic field of the primary transponder 15 and thereby greatly reduces unauthorised code reading. In addition the key holder can be moved to a normal usable position (fig 3) whereby the electromagnetic shield and second transponder are displaced from the primary transponder to allow the code to be clearly read by an authorised code reader.

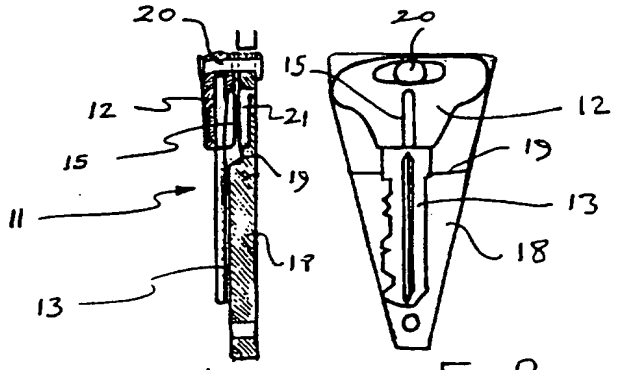

Fig 1

Fig 2

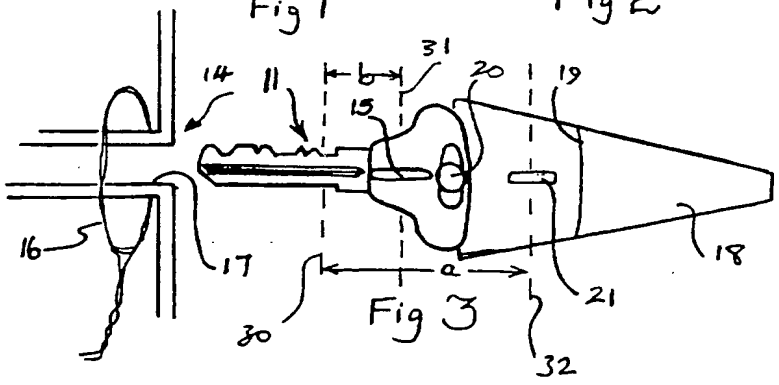

Fig 3

GB 2 294 720 A

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

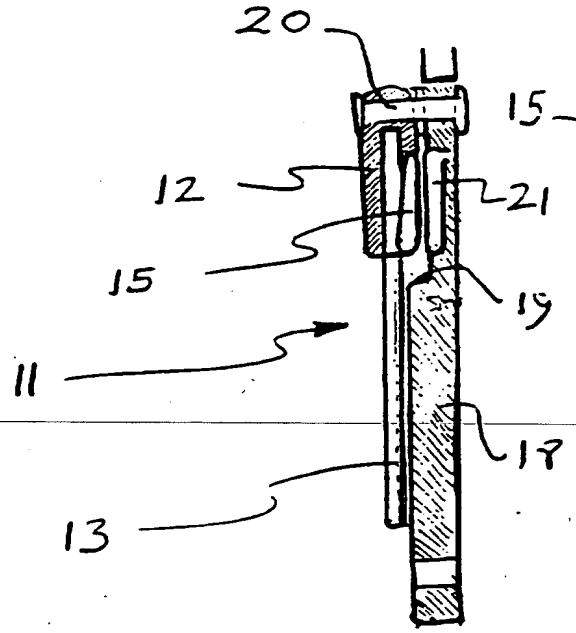

Fig 1

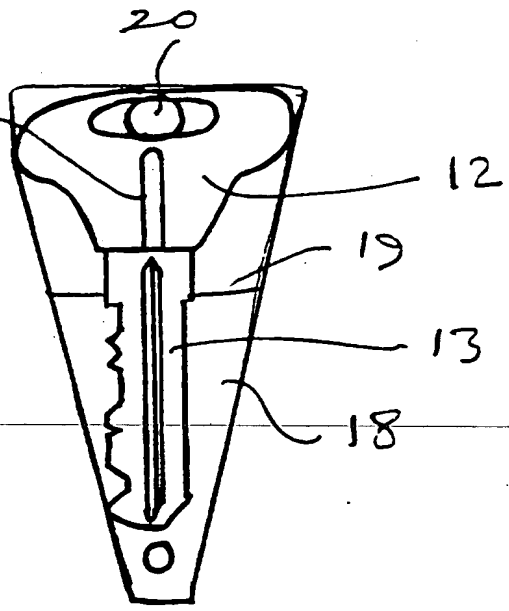

Fig 2

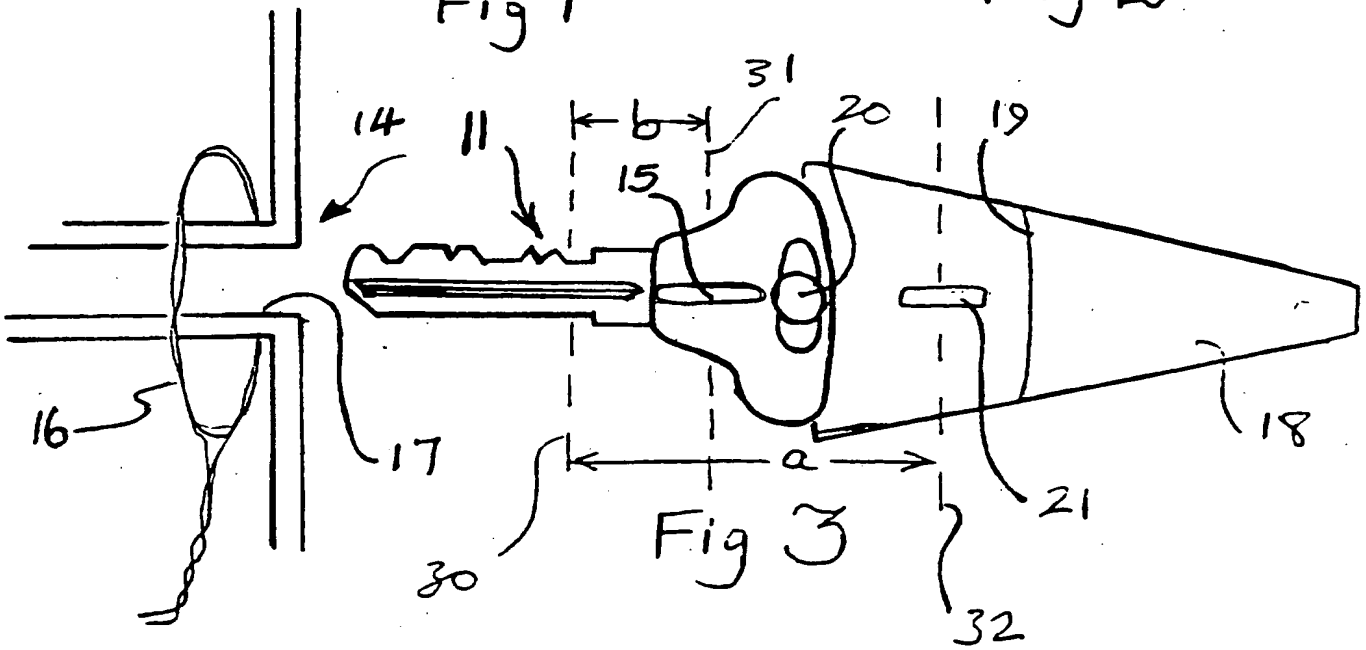

Fig 3

A KEY HOLDER

The present invention relates generally to a key holder, and specifically to a key holder having special features for use in a security system.

Although mechanical key and lock combinations have been used for centuries to provide security against unauthorised entry or operation of equipment, mechanical locks have serious disadvantages in providing only a limited number of alternative combinations or "codes" in being relatively easily circumvented by skilled lock pickers, or even forced by use of crude instruments capable of stressing the mechanical components beyond their limits of resistance.

Additional security is frequently sought by having recourse to electronic systems in which coded signals can be transmitted between a "key" and a lock which signals operate on a remote control unit which then determined whether the lock is released electrically. Known such electronic control units include systems for radiating coded signals carried at infra red wave lengths, or radiating signals at radio frequencies.

One disadvantage of electronic systems lies in the necessity of transmitting a coded signal across space, however small, between the key and the lock. This weak

link can be exploited by the unprincipled to gain access to the security code by detecting it during transmission. This can be done utilising equipment sensitive to reflected radiations in the case of infra red transmitters, or may be achieved by scanning a number of frequencies in the case of radio frequency transmitters. By gaining close proximity to a key containing a security code, even though it may be in the user's pocket, an unauthorised person may be able to extract the information identifying the key by radiating a signal varying in time and locating the carrier frequency at which the key oscillates and recording the coded signal thus retransmitted.

Typically, such radio frequency systems involve the use of so-called transponders, which comprise an antenna coil connected to a circuit made utilising modern integrated circuit (chip) technology which requires very low power and can, in fact, be energised by the electrical power sensed by the coil. Of course such systems have a very short range, but this is nevertheless within the bounds of practicality since, in practice, key and lock combinations are generally required to work in cooperation when in relatively close proximity. In this connection, radio frequency or microwave frequency transponders may have a range of several tens of metres if adequately powered, although certain restrictions apply to the energy density which can be radiated in a

public space resulting in the production of systems which usually have a rather shorter range, say in the region of 1 metre or less.

Even at very short range, such as the centimetre range, a scanner could be used to extract coded information from a RF or microwave transponder and the present invention addresses the problem of ensuring that a transponder unit is adequately protected from unauthorised extraction of information.

In one aspect of the present invention, therefore, there is provided a holder for a key of the type having a reactive device such as an RF or microwave transponder, responsive to a radiated electromagnetic signal, in which there is provided a second reactive device in close physical proximity to the transponder when the key is in a first relative position with respect to the holder such that the second reactive device reacts to and influences a radiation field at substantially the same frequency or within the same frequency range.

In this way, when the key is in the holder any attempt to extract the coded information by unauthorised radiation of a carrier and scanning the likely frequency ranges is frustrated by the "jamming" effect of the second transponder. In use, however, when the key is removed by the authorised holder and inserted into a lock the

reactive unit of the key is then sufficiently far away from that on the holder for no confusion of the signals to occur.

In a preferred embodiment the said reactive device and/or the second reactive device preferably has an antenna coil and an integrated circuit unit (preferably of the one time programmable type) operable to react to an applied carrier signal within a given frequency range so as to introduce temporal variations in the effective inductance of the reactive device thereby re-radiating a signal detectable by a sensing antenna within a limited range thereof.

The said coil antenna of the said second reactive device may be a flat plain coil lying in a plane substantially parallel to that in which the body of the key lies when in the holder, or may be a small cylindrical coil having an access parallel to that of the antenna of the said reactive device.

In this latter case the holder may be provided with pivotal connection means for pivotally connecting a key to the body of the holder in such a way that the key can turn, with respect to the holder, between the said first relative position of key and holder and a second relative position thereof.

The holder may enclose the key, or may simply secure it alongside the holder body. Typically, the holder may be a substantially planar substantially rigid member against which the key may be located when in the said first relative position. To retain the key on the holder there may be provided snap engagement locating means, which also determine the position of the key with respect to the holder in the said first relative position thereof.

Naturally, the said second reactive device preferably responds to substantially the same stimulating frequency as the said reactive device although, for convenience, it may respond to a slightly different carrier frequency, whereas the response of the second reactive device is preferably entirely unrelated to the response of the said reactive device such that, when the key is in the said first position with respect to the holder and subject to stimulating radiation within the said frequency range to which the said reactive device responds, the joint or resultant response of the two said reactive devices masks the individual response of either device and especially that of the said reactive device.

Alternatively, the response of the said second reactive device may be related to that of the said reactive device, but in such a way that the components of the joint or resultant response are effectively indistinguishable. Any attempt to scan the reactive

device to extract its code will therefore be frustrated when the key is in the holder. Of course, the holder may simply define a pocket into which at least a part of the key can be introduced in order to determine the said first relative position of key and holder, and the key may be entirely removable from the holder for insertion into a lock.

One embodiment of the present invention will now be more particularly described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a sectional view, taken on the line I-I of Figure 2, illustrating a key holder formed as an embodiment of the present invention;

Figure 2 is a frontal view of a holder carrying a key seen from the arrow II of figure 1; and

Figure 3 is a view of the holder and key combination illustrated in Figures 1 and 2 shown in its position of use.

Referring now to the drawings, there is shown a key generally indicated 11 having a key body 12 and a key blade 13. The blade 13 is entirely conventional, having a notched edge for mechanical interaction with tumblers (not shown) in a lock generally indicated 14 in Figure 3.

Housed within the key body 12 is a one time programmable ID tag device, which may be for example of the type sold

as an ID tag by Nexus Limited, and which comprises a small cylindrical coil connected electrically to an integrated circuit which requires very low power, which can be derived from the coil when this is resonated by an applied carrier wave signal at an appropriate resonant frequency. Typically the resonant frequency may be in the region of 125 KHz. The OTP device operates, when activated, to vary the inductants of the coil thereby changing the flux linkage with a radiating source (in this case a coil 16 around a lock opening 17 in the lock 14 into which the key is inserted to operate the lock) allowing this to be detected by electronic circuitry connected to the coil 16. The OTP device has a unique code stored within it which determines the temporal variation of inductants changes thereby effectively giving a unique signal identifying itself to the electronic circuitry associated with the coil 16.

Typically, the range over which such inductants linkage is sufficiently great to provide detectable signals over the noise present due to variations induced in the coil 16 by its passage through the earth's magnetic field and/or the transition of energetic particles normally present in the atmosphere, is of the order of only a few millimetres so that the coil 16 detects the presence of the OTP device 15 only once the key is inserted fully into the opening 17.

In order to prevent scanning of the key by unauthorised persons, for example when in the authorised user's pocket, the key is provided with a holder in this embodiment in the form of a substantially triangular rigid plate 18 having a shouldered recess 19 for receiving the body 12 of the key and a pivot pin 20 by which the key is pivoted (preferably rivetted) to the holder 18. embedded within the holder 18 is a second OTP device 21 which, when the key is in the storage position on the holder 18 as illustrated in Figures 1 and 2, lies closely adjacent to the key's own OTP device 15. In the presence of a stimulating radiation field in or close to the range of resonant frequencies of the coil the OTP device 21 also acts to reradiate a signal effectively by varying the inductance of the coil, and the pattern of variations in this case is entirely unrelated to the pattern of variations caused by the key's OTP device. Information concerning the code stored in the OTP device 15 cannot therefore be established.

In use, however, the holder 18 is swung around the pivot 20 to a position where, as shown in Figure 3, the holder's OTP device 21 is spaced from the OTP device 15 on the key by a distance greater than the sensitivity range of the coil 16. As can be seen in Figure 3 the working distance between the coil 16 the position of which is shown by the broken line 30 in Figure 3, is approximately b (the mid line of the OTP device 15 being

identified by the broken line 31). By contrast the distance a from the coil's position 30 to the mid line, indicated by the broken line 32, of the holder's OTP device 21 is more than twice this distance and greater than the limited range within which either the OTP device 21 will resonate at the frequency transmitted by the coil 16 (because of the inverse square reduction in field strength) and certainly greater than the range at which the coil 16 will "see" the OTP device 21. Operation of the key 11 in the lock 14 is therefore unaffected.

CLAIMS

1. A transponder key holder for systems in which a transponder is provided with electronic storage means for storing information in the form of electronically readable code that can be detected upon approach or insertion of an attached key, whereupon the key holder provides a means by which the coded information is protected from unauthorised code reading by way of an electromagnetic shield as part of the key body and holder, and by a second transponder that serves to interfere with the electromagnetic field of the primary transponder and thereby greatly reduces the probability of obtaining the correct code (to enable a system), additionally the transponder key holder is provided with a normal usable position whereby the electromagnetic shield and second transponder are rotated or displaced to allow the codes from the primary transponder to be clearly read by an authorised code reader.

2. A transponder key holder for systems as claimed in 1 which the electronically stored information within a primary transponder is protected from unauthorised reading by the body of the key and/or holder.

3. A transponder key holder for systems as claimed in 1 in which the electronically stored information within a primary transponder is protected is protected from unauthorised reading by a second transponder that when energised, generates an electromagnetic field that swamps or simply interferes with the primary transponder's fields.

4. A transponder key holder for systems as claimed in 3 in which a transponder maybe protected by a similar device mounted in close proximity.

5. A transponder key holder for systems as claimed in 1 in which a transponder is used in a security system that relies on the generation of electronic codes that protect an enable plant, machinery, vehicles, buildings, equipment or devices.

6. A transponder key holder for systems as claimed in 5 in which enablement is made when the primary transponder is placed in close proximity with the axis of rotation parallel with that of a coil (or similar) antenna and with the axis of the second transponder substantially at right angles to the axis of rotation.

7. A transponder key holder for systems as claimed in 1 in which the primary transponder may be mounted on a key of a mechanical lock, whereby the axis of rotation and distance from the (coil) antenna is defined by the blade of the key in relation with the lock.

2.

8. A transponder key holder for systems as claimed in 1 in which OTP or Read/Write Programmable Transponders are protected by transponders that use a similar modulation and demodulation technique (such as AM,FM,AMSK,FSK and PSK).

9. A transponder key holder for systems as claimed in previous claims (1 to 8) in which the basic elements are assembled to form an elegant item that is easily carried but includes the essential features that allow normal functions and protective use.

10. A transponder key holder substantially as described herein with reference to Figures 1 - 3 of the accompanying drawings.

Patents Act 1977 **Examiner's report to the Comptroller under Section 17** **(The Search report)**	Application number GB 9418887.7
Relevant Technical Fields (i) UK Cl (Ed.O) E2A (AEE) (ii) Int Cl (Ed.6) E05B (19/00, 49/00)	Search Examiner P J SILVIE Date of completion of Search 18 JANUARY 1996
Databases (see below) (i) UK Patent Office collections of GB, EP, WO and US patent specifications. (ii) ONLINE: WPI	Documents considered relevant following a search in respect of Claims :- ALL

Categories of documents

X:	Document indicating lack of novelty or of inventive step.	**P:**	Document published on or after the declared priority date but before the filing date of the present application.
Y:	Document indicating lack of inventive step if combined with one or more other documents of the same category.	**E:**	Patent document published on or after, but with priority date earlier than, the filing date of the present application.
A:	Document indicating technological background and/or state of the art.	**&:**	Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages	Relevant to claim(s)
	NONE	

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).